protiviti®
Global Business Consulting

Board Perspectives

ISSUE 193

Near-Term Risk Outlook: Directors vs. Management

As in prior years, our most recent annual survey of leaders contrasts the perspectives of active directors with C-level executives regarding the 2026 risk landscape. This year, we also asked how they prioritise investments to address risk.

Conducted during the fall of 2025 in partnership with NC State University's Enterprise Risk Management Initiative, our survey captures insights from 1,540 C-level executives and directors regarding their perspectives on the top risks over the near-term (two to three years ahead). Geographically, 35% of the survey participants represent companies based in North America, 31% in Europe, 24% in the Asia-Pacific region, and the remaining 10% from Latin America, the Middle East, India and Africa. The survey provides a useful forum for contrasting the views of close to 100 directors with the views of C-level executives regarding the risk landscape for the next two to three years.

The risk landscape: A director's perspective

In the accompanying table (see next page), the 10 highest-rated risk themes noted in our survey by the participating directors are listed in order of priority to provide a context for understanding the most critical uncertainties companies face over the next two to three years. These risks were prioritised by the directors rating the impact of 28 specific risks across three dimensions — macroeconomic, strategic and operational.

In reviewing this list, the directors are:

Concerned with cyber threats. As the top risk, cyber threats are existential rather than just technical issues. Accordingly, cyber resilience and cyber risk metrics must be embedded into enterprise strategy and boardroom performance dashboards. The recent Mythos threat has ushered in a new sense of urgency to identify and fix vulnerabilities before threat actors exploit them.

Focused on talent and skills. Four of the top six risks relate to human capital. Inability to attract/retain talent and skills and succession challenges are key concerns from the standpoint of building and sustaining the executive bench strength so critical to long-term success. So is the availability of talent and skills necessary to sustain the business, as it fuels competition for talent and increases personnel costs. Finally, adoption of digital technologies alters the skills profile needed to fully realise the value proposition promised by these new capabilities. These new skills are in short supply, requiring significant investments in upskilling and reskilling.

Watching the economy closely. Economic uncertainty remains a critical concern and merits close attention. While fiscal policies and deregulatory trends in the United States and the huge spend on artificial intelligence (AI) infrastructure have stimulated the economy, there are other moving parts contributing to uncertainty going forward. For example, consumer behaviour, inflation trends, central bank policy shifts, geopolitical developments (including regional conflicts, such as with the Iranian war and in Ukraine), global supply chain adjustments, AI-driven productivity gains, trade policy, and labour market effects are impactful considerations. In this interconnected world, events often affect economies. Indeed, regional conflicts, supply-side shocks, tariff uncertainty and persistent price pressures in certain sectors have fuelled inflation, particularly in the United States.

Prioritising sustaining competitiveness. Three concerns in the top 10 risks noted by directors support this theme. First, new and emerging technologies and other market forces are driving disruptive change. Second, outdated legacy IT infrastructure systems and insufficient digital capabilities are hindering the innovation needed to remain competitive. Finally, the regulatory climate is a major factor for multinationals, as regulatory changes and oversight in different jurisdictions can affect how processes are designed and products and services are produced and delivered. For example, the European Union recently adopted its landmark AI

Top near-term risks: directors

1. Insufficient preparations to manage cyber threats that could disrupt operations or damage the brand
2. Inability to attract/retain talent, manage shifts in labor expectations and address succession challenges
3. Lack of availability of the talent and skills needed to sustain the business
4. Economic conditions, including inflationary pressures, restrict growth, impact margins or require new skills
5. Anticipated increases in labor costs may affect ability to meet profitability targets
6. Adoption of new and emerging technologies elevating the need to upskill/reskill our workforce
7. Regulatory changes/scrutiny affect process design and product/service production and delivery
8. Compliance with growing data privacy regulations may require significant resources
9. Existing legacy IT infrastructure limits competitiveness with "born digital" or modernising players
10. Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces

Act, providing a framework for the regulation and ethical deployment of AI. In addition, major antitrust lawsuits and regulatory actions have targeted large technology companies in the United States, the EU and Asia.

Not forgetting privacy risks. Boards have grappled with privacy concerns for a long time. Despite the fatigue, compliance with growing data privacy regulations may require significant resources in managing how data is collected, processed, used and stored.

The risk landscape: A management perspective

Over 60 CEOs responded to our survey. Their view of the risk landscape is very similar to that of the participating directors, although their ranking of the risks is different. There are two highly relevant risks they included in their top 10 risks looking out two to three years that the directors did not cite:

- **Geopolitical shifts, regional conflicts and unstable governments.** Geopolitical tensions continue to stir uncertainty in global markets, forcing organisations to pivot and adapt to new business realities. Diversifying supply chains, nearshoring, reshoring, monitoring global developments — creating resilient global strategies is a dynamic ball game. Iran's shutdown of the Strait of Hormuz illustrates the potential impact of how geopolitical developments can bring about an abrupt cessation of a vital supply chain system.
- **Sustaining customer loyalty and retention.** Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences for different products, services and buying experiences. The picture is complicated by ongoing demographic shifts in the customer base.

As for CEO direct reports (CFOs, COOs, CTOs/CIOs and CHROs), 900 responded to our survey. They included three risks that are not mentioned above:

- **Reliance on third-party vendors and ecosystem partners.** These executives spend a lot of time with these parties and know that third-party risk introduces systemic vulnerabilities. For example, the lack of visibility into vendor practices, especially in multitiered supply chains and cloud-based services, can further complicate cyber threats and highlight the fragility of IT infrastructures and the need for

Iran's shutdown of the Strait of Hormuz illustrates the potential impact of how geopolitical developments can bring about an abrupt cessation of a vital supply chain system.

robust governance across a multiplicity of attack vectors in the extended enterprise.

- **Emergence of new risks from implementing AI.** Adoption of AI continues to accelerate as concerns about ethical and responsible deployment, regulatory uncertainty and operational disruption grow. Senior executives know they need a robust governance framework and cross-functional oversight to identify, track and manage the evolving risks associated with AI deployments.
- **Changes in global markets and trade policies.** These challenges are understandable, as they can be correlated with the concerns expressed earlier regarding the economy and geopolitical tensions.

More than 240 executives in second line functions (CISOs, CROs and CCOs) also participated in our survey. Their top 10 risks align to those mentioned above. Likewise, the more than 170 third line function executives (CAEs) who participated in our survey reported top 10 risks that included risks discussed earlier.

What are the next steps?

We asked our survey participants to identify the top three strategic investment priorities, in rank order, in which their organisations are likely to invest over the next two to three years. We provided them a list of 12 investment areas that relate to some of the strategic and operational near-term risk issues our survey examined. Seven of these investment areas figured prominently in the survey findings.

The table on the following page summarises the investment priorities for directors, CEOs and the other three groups of management. For CEO direct reports and second line executives, the table lists all priorities identified by each type of executive included in the category rather than the top three priorities for the category as a whole.

Senior executives know they need a robust governance framework and cross-functional oversight to identify, track and manage the evolving risks associated with AI deployments.

Investment priority	Directors	CEO	CEO directs	Second line	Third line
Business process improvements	x	x	x	x	x
Cybersecurity			x	x	x
Customer experience	x	x			x
Infrastructure modernisation			x	x	
Data privacy			x		
Human capital management	x	x	x		
Regulatory compliance infrastructure			x	x	

The above priorities offer insights as to where directors and management are likely to invest in addressing the various risks they identified in the survey, not to mention opportunities they envision over the next two to three years. Following is some commentary on the above table:

- **Directors and CEOs are on the same page.** It is interesting that directors ranked customer experience as an investment priority when they did not include customer loyalty and retention as a top 10 near-term risk. This apparent incongruence is likely due to their considering such investments a strategic opportunity. This emphasis at the top sets a tone on execution and impact with a focus on how the organisation operates and its capability to deliver superior outcomes.
- **CEO direct reports are focused on operational excellence with a "protect the fortress" strategy.** To illustrate, for CFOs, the top three priorities are data privacy, cybersecurity and infrastructure modernisation — suggesting a focus on fiduciary duty. COOs also prioritised these three areas, which makes sense, as system stability and data integrity are prerequisites for reliable operations. Understandably, CTOs/CIOs listed data privacy, cybersecurity and regulatory compliance, and CHROs cited human capital management and skilling, followed by business process improvements.
- **Second line and third line leaders are focused on cybersecurity and business process improvements.** There are, of course, some variations. CISOs are concerned with data privacy and regulatory compliance. Interestingly, CROs and CCOs see infrastructure modernisation as a priority. CAEs rate customer experience as a top priority.

Thus, it appears the oversight, control and assurance functions are interested in the areas most critical for risk reduction, with emphasis on securing systems and ensuring that underlying processes and platforms are relevant, stable, reliable and resilient.

Key takeaways for the board

There is general agreement among directors, CEOs and varying levels of management as to the most significant risks looking out two to three years. However, the variability in ranking the risks suggests the need for diverse voices at the table when enterprise risks are assessed. Likewise, because most organisations have finite resources, the divergent thinking around investment priorities necessitates a collaborative approach that invites a broad range of perspectives.

For boards, these shared risk signals should be translated into disciplined governance. For example:

- Be mindful of the CEO's concerns, particularly those relating to the customer experience.
- Keep an eye on global developments, as they can drive a board and management team to pivot over a very short period of time.
- Confirm management has clear ownership, metrics and reporting for cyber resilience and data privacy, and is identifying and addressing software and data vulnerabilities in a timely manner.
- Pressure-test the talent strategy (including succession depth and critical skill gaps) to ensure this strategic imperative is delivering to expectations.
- Oversee plans to modernise legacy technology and business processes that currently constrain innovation, cybersecurity and competitiveness.
- Ensure risk governance extends across third parties and new AI deployments through explicit policies, controls and cross-functional oversight.

The divergent thinking around investment priorities necessitates a collaborative approach that invites a broad range of perspectives.

Finally, boards should use the differing rankings across constituencies as a prompt to broaden the voices informing the enterprise risk assessment process and to align capital and operating investments to the vital few priorities that will most improve resilience and performance over the next two to three years.

For more information concerning our study, explore the full results of our Top Risks and Opportunities Survey. In addition to insights regarding near-term risks and strategic investments, our research provides perspectives on growth, opportunities and challenges associated with the transformative impact of AI, and the top risks on the horizon over the long-term (a decade from now).

About the authors

Matthew Moore
Managing Director, Protiviti

Matt is a Managing Director and Global Leader of Protiviti's Legal, Risk & Compliance practice, helping organisations modernise and strengthen their risk capabilities. Matt is also the Global Head of Solution Enablement at Protiviti. He has extensive experience advising clients on regulatory compliance, corporate governance and internal controls, with a focus on building risk appetite frameworks, advancing governance maturity and enhancing executive-level risk reporting.

Contact Matt at **matthew.moore@protiviti.com**.

Jim DeLoach
Managing Director, Protiviti

Jim DeLoach is a founding Managing Director at Protiviti. Based in Houston, he is well known for his commentary on many governance topics.

Contact Jim at **jim.deloach@protiviti.com**.

Protiviti (**www.protiviti.com**) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit — enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the **Fortune 100 Best Companies to Work For®** list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

protiviti®